

Polar Coding for the General Wiretap Channel

Yi-Peng Wei Sennur Ulukus

Department of Electrical and Computer Engineering
University of Maryland College Park, MD 20742
ypwei@umd.edu ulukus@umd.edu

Abstract—Information-theoretic work for wiretap channels is mostly based on random coding schemes. Designing practical coding schemes to achieve information-theoretic security is an important problem. By applying the two recently developed techniques for polar codes, we propose a polar coding scheme to achieve the secrecy capacity of the general wiretap channel.

I. INTRODUCTION

The wiretap channel was first introduced by Wyner [1], in which a legitimate transmitter (Alice) wishes to send messages to a legitimate receiver (Bob) secretly in the presence of an eavesdropper (Eve). Wyner [1] characterized the capacity equivocation region for the degraded wiretap channel, in which the received signal at Eve is a degraded version of the received signal at Bob. Later, Csiszár and Körner [2] characterized the capacity equivocation region for general, not necessarily degraded, wiretap channels. These works are based on information-theoretic random coding schemes.

Polar coding, invented by Arıkan [3], is the first code that provably achieves the capacity of the binary-input discrete symmetric output channels (B-DMC). The idea of polar coding has been extended to lossless source coding [4], lossy source coding [5], and to multi-user scenarios, such as, multiple access channel [6]–[8], broadcast channel [9], [10], interference channel [11], and Slepian-Wolf coding problem [12].

On a B-DMC, polarization results in two kinds of sub-channels [3]. The first kind is good sub-channels. The capacity for these sub-channels approaches 1 bit per channel use. The second kind is bad sub-channels. The channel output for these sub-channels is independent of the channel input; therefore the capacity for these sub-channels approaches 0. In particular, if a B-DMC A is degraded with respect to a B-DMC B, then the good sub-channels of A must be a subset of the good sub-channels of B [13]. We call this the *subset property*.

Polar coding schemes for *degraded* wiretap channels with *symmetric* main and eavesdropper channels are developed using the subset property in [14]–[17]. For degraded wiretap channels, the good sub-channels of Eve is a subset of the good sub-channels of Bob. The polar coding scheme is designed to transmit the confusion messages (random bits) on the sub-channels simultaneously good for Bob and Eve, and to transmit the secret messages on the sub-channels only good for Bob. However, for non-degraded wiretap channels, the subset property no longer holds [18]–[22], i.e., the good sub-channels of

Eve is not necessary a subset of the good sub-channels of Bob. Moreover, the secrecy capacity achieving input distribution is not necessarily a uniform distribution. Therefore, the polar coding schemes in [14]–[17] cannot directly extend to the non-degraded wiretap channel.

By applying the two recently developed techniques for polar codes, we can achieve the secrecy capacity of the general wiretap channel. The first is universal polar codes [21], [22]. Universal polar coding allows us to align the good sub-channels of Bob and Eve together. Therefore, we can artificially construct the subset property for the non-degraded wiretap channel. Then, Alice transmits the random bits on the sub-channels simultaneously good for Bob and Eve, and the secret message on the sub-channels only good for Bob. The second is polar coding for asymmetric models [23], which allows us to deal with the non-uniform input distribution. Different from B-DMC, polarization for asymmetric channel results in three different kinds of sub-channels.

Another polar coding scheme for the general wiretap channel is provided in [24], which uses a concatenated code consisting of two polar codes. The inner layer ensures that the transmitted message can be reliably decoded by Bob, and the outer layer guarantees that the message is kept secret from Eve. Our work jointly handles these two goals in one shot. Hence, the decoding error probability of our scheme is approximately $O(2^{-n^{1/2}})$, whereas it is $O(\sqrt{n}2^{-n^{1/4}})$ in [24]. Moreover, for practical code construction, there is still no efficient way to characterize the outer index set [24, Sec III. C.], while our coding scheme can be efficiently constructed by [19].

II. WIRETAP CHANNEL MODEL

A wiretap channel consists of a legitimate transmitter (Alice) who wishes to send messages to a legitimate receiver (Bob) secretly in the presence of an the eavesdropper (Eve). The channel between Alice and Bob is called the main channel, and the channel between Alice and Eve is called the eavesdropper channel. Let X denote the single-letter input to the main and eavesdropper channels. Let Y and Z denote the corresponding single-letter outputs of the main and the eavesdropper channels, respectively. W represents the message to be sent to Bob and kept secret from Eve with $W \in \mathcal{W} = \{1, \dots, 2^{nR}\}$. Let $P_e = \Pr(\hat{W} \neq W)$ denote the probability of error for Bob's decoding.

The equivocation rate is given by $\frac{1}{n}H(W|Z^n)$, which reflects the uncertainty of the message given eavesdropper's channel observation. A rate-equivocation pair (R, R_e) is

achievable if as $n \rightarrow \infty$, $P_e \rightarrow 0$ and $\lim_{n \rightarrow \infty} \frac{1}{n} H(W|Z^n) \geq R_e$. Perfect (weak) secrecy is achieved if $R = R_e$ [2]. Therefore, perfect secrecy is achieved if $\frac{1}{n} I(W; Z^n) \rightarrow 0$, and the *secrecy capacity* C_s is the highest achievable perfect secrecy rate R , which is also the highest possible equivocation rate [2]. Csiszár and Körner characterized the secrecy capacity for the general wiretap channel, which is [2]

$$C_s = \max_{V \rightarrow X \rightarrow Y, Z} I(V; Y) - I(V; Z). \quad (1)$$

In the following, we assume that we already know the optimal input distribution [25], i.e., we know the optimal V , X that achieve C_s . Although we focus on developing a coding scheme for binary inputs below, there is no difficulty to extend the work to q -ary inputs [26]–[29].

III. POLAR CODES

A. Polar Codes for Asymmetric Channels

Let P_{TV} be the joint distribution of a pair of random variables (T, V) , where T is a binary random variable and V is any finite alphabet random variable. Let us define the Bhattacharyya parameter as follows

$$Z(T|V) = 2 \sum_v P_V(v) \sqrt{P_{T|V}(0|v) P_{T|V}(1|v)}. \quad (2)$$

Let $U^n = X^n G_n$, where X^n denotes n independent copies of the random variable X with $X \sim P_X$, and $G_n = G^{\otimes k}$ where $G = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and \otimes denotes the Kronecker product of matrices for $n = 2^k$. [4] shows as $n \rightarrow \infty$, U_i is almost independent of U^{i-1} and uniformly distributed, or otherwise U_i is almost determined by U^{i-1} . Therefore, $[n]$, the index set $\{1, 2, \dots, n\}$, is almost polarized into two sets \mathcal{H}_X and \mathcal{L}_X :

$$\begin{aligned} \mathcal{H}_X &= \{i \in [n] : Z(U_i|U^{i-1}) \geq 1 - \delta_n\} \\ \mathcal{L}_X &= \{i \in [n] : Z(U_i|U^{i-1}) \leq \delta_n\}, \end{aligned} \quad (3)$$

where $\delta_n = 2^{-n^\beta}$ and $\beta \in (0, 1/2)$. Moreover,

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{H}_X| &= H(X) \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_X| &= 1 - H(X). \end{aligned} \quad (4)$$

Let P be a discrete memoryless channel with a binary input X and finite alphabet output Y . Here, P does not have to be a symmetric channel. Fix a distribution P_X for X . [23] generalizes the above argument to achieve a rate close to $I(X; Y)$. Consider two subsets of $[n]$, $\mathcal{H}_{X|Y}$ and $\mathcal{L}_{X|Y}$, defined as follows

$$\begin{aligned} \mathcal{H}_{X|Y} &= \{i \in [n] : Z(U_i|U^{i-1}, Y^n) \geq 1 - \delta_n\} \\ \mathcal{L}_{X|Y} &= \{i \in [n] : Z(U_i|U^{i-1}, Y^n) \leq \delta_n\}, \end{aligned} \quad (5)$$

similar to (4), we have

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{H}_{X|Y}| &= H(X|Y) \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{L}_{X|Y}| &= 1 - H(X|Y). \end{aligned} \quad (6)$$

With (3) and (5), we define the following three sets

$$\mathcal{I} = \mathcal{H}_X \cap \mathcal{L}_{X|Y} \quad (7)$$

$$\mathcal{F}_r = \mathcal{H}_X \cap \mathcal{L}_{X|Y}^c \quad (8)$$

$$\mathcal{F}_d = \mathcal{H}_X^c. \quad (9)$$

In the following, we call the set \mathcal{I} the *information set*, and sets \mathcal{F}_r and \mathcal{F}_d the *frozen set*. Although we call them the *frozen set*, \mathcal{F}_r and \mathcal{F}_d have different operational meanings which will be illustrated below. Note that for the symmetric channel capacity achieving code design, \mathcal{F}_d is an empty set [3].

To achieve rate $I(X; Y)$ for channel P , let us consider the following coding scheme. First, the encoder transmits the information bits in the index set \mathcal{I} . For $i \in \mathcal{I}$ in (7), since $i \in \mathcal{H}_X$, U_i is almost independent of U^{i-1} and uniformly distributed. Therefore, the encoder can freely assign values to $U_{\mathcal{I}}$, where $U_{\mathcal{I}}$ denotes a sub-vector $\{U_i\}_{i \in \mathcal{I}}$. Moreover, since $i \in \mathcal{L}_{X|Y}$, U_i is almost determined by U^{i-1} and Y^n , which means that given the channel output Y^n , U_i is decoded in a successive manner.

Second, for $i \in \mathcal{F}_r$ in (8), U_i is almost independent of U^{i-1} and uniformly distributed, and given the channel output Y^n , U_i cannot be reliably decoded. The encoder transmits $U_{\mathcal{F}_r}$ with a uniformly random sequence and the randomness is shared between the transmitter and the receiver.

Last, for $i \in \mathcal{F}_d$ in (9), U_i is almost determined by U^{i-1} . The values of $U_{\mathcal{F}_d}$ are computed in successive order through the following randomized map

$$u_i = \arg \max_{u \in \{0,1\}} P_{U_i|U^{i-1}}(u|u^{i-1}). \quad (10)$$

By (4) and (6), it is easy to verify that

$$\lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{I}| = I(X; Y). \quad (11)$$

Moreover, by applying successive cancellation decoder, the block error probability P_e can be upper bounded by

$$P_e \leq \sum_{i \in \mathcal{I}} Z(U_i|U^{i-1}, Y^n) = O(2^{-n^\beta}) \quad (12)$$

for any $\beta \in (0, 1/2)$, with complexity $O(n \log n)$. Therefore, the rate $I(X; Y)$ is achieved.

B. Universal Polar Coding

Consider two B-DMCs $P : X \rightarrow Y$ and $Q : X \rightarrow Z$, and assume that these two channels have identical capacities, i.e., $C(P) = C(Q)$. Let $U^n = X^n G_n$, and denote \mathcal{P} and \mathcal{Q} as the information set defined in (7), i.e.,

$$\mathcal{P} = \{i \in [n] : Z(U_i|U^{i-1}, Y^n) \leq \delta_n\}$$

$$\mathcal{Q} = \{i \in [n] : Z(U_i|U^{i-1}, Z^n) \leq \delta_n\},$$

where $\delta_n = 2^{-n^\beta}$ and $\beta \in (0, 1/2)$. Since we assume $C(P) = C(Q)$, we also have $|\mathcal{P}| = |\mathcal{Q}|$.

In general, the differences $\mathcal{P} \setminus \mathcal{Q}$ and $\mathcal{Q} \setminus \mathcal{P}$ are not empty sets [18]–[20]; therefore, it is not straightforward to apply standard polar coding to achieve the capacity of the compound

channel consisting of P and Q . [21] proposes a method, called *chaining construction*, to solve this problem.

Definition 1 (*Chaining construction [21]*) Let $m \geq 2$. The m -chain of \mathcal{P} and \mathcal{Q} is a code of length mn that consists of m polar blocks of length n . In each of the m blocks, the set $\mathcal{P} \cap \mathcal{Q}$ is set to be an information set. In the i th block, $1 \leq i < m$, the set $\mathcal{P} \setminus \mathcal{Q}$ is also set to be an information set. Moreover, the set $\mathcal{P} \setminus \mathcal{Q}$ in the i th block is chained to the set $\mathcal{Q} \setminus \mathcal{P}$ in the $(i+1)$ th block in the sense that the information is repeated in these two sets. All other indices are frozen. Therefore, in each block, the set $(\mathcal{P} \cup \mathcal{Q})^c$ is frozen, and the set $\mathcal{Q} \setminus \mathcal{P}$ in the 1st block and the set $\mathcal{P} \setminus \mathcal{Q}$ in the m th block are frozen, too. Note that $(\cdot)^c$ denotes the complement of a set. The rate of the chaining construction is

$$\frac{|\mathcal{P} \cap \mathcal{Q}| + \frac{m-1}{m}|\mathcal{P} \setminus \mathcal{Q}|}{n}. \quad (13)$$

Next, we discuss the decoding procedure for the compound channel consisting of P and Q . If the channel P is used, then we decode from the first block. On the other hand, if the channel Q is used, then we decode from the last block.

First, suppose that channel P is used and a code of length mn has been received. For this case, we decode from the first block. In the 1st block, we put all the information bits in the set \mathcal{P} , thus the decoder can decode correctly. For the 2nd block, through chaining construction, the set $\mathcal{P} \setminus \mathcal{Q}$ in the 1st block is chained to the set $\mathcal{Q} \setminus \mathcal{P}$ in the 2nd block, and the set $(\mathcal{P} \cup \mathcal{Q})^c$ is frozen. Equivalently, the decoder only needs to decode the bits in the set \mathcal{P} , which can be correctly decoded. The same procedure holds until the $(m-1)$ th block. For the m th block, the information bits are only put in the set $\mathcal{P} \cap \mathcal{Q}$, and the remaining part has been determined. Hence, information bits can be reliably decoded. The main rate loss for the chaining construction comes from the last block.

Second, consider the case that the channel Q is used. In this case, we decode from the last block. In the m th block, since the information bits are put in the set \mathcal{Q} , reliable decoding is guaranteed. For the $(m-1)$ th block, due to the chaining process, the set $\mathcal{Q} \setminus \mathcal{P}$ in the m th block is chained to the set $\mathcal{P} \setminus \mathcal{Q}$ in the $(m-1)$ th block, and note that the set $(\mathcal{P} \cup \mathcal{Q})^c$ is frozen. The decoder only needs to decode the information bits in the set \mathcal{Q} , thus correct decoding is ensured. This procedure is applied until the 2nd block. For the 1st block, information bits which have not been determined fall in the set $\mathcal{P} \cap \mathcal{Q}$, thus the decoder can decode them correctly.

In summary, for a fixed m , if we let $n \rightarrow \infty$, we can achieve the rate in (13) with arbitrary small error probability, which also means that the rate $C(P) - \frac{1}{m} \frac{|\mathcal{P} \setminus \mathcal{Q}|}{n}$ can be achieved. Additionally, if we let $m \rightarrow \infty$, then the rate $C(P)$, which is the capacity of the compound channel consisting of channels P and Q , can be achieved.

IV. POLAR CODING FOR THE GENERAL WIRETAP CHANNEL

Assume now that we know the optimal distributions to achieve the secrecy capacity C_s in (1), i.e., we know the

optimal V and X . For illustration, we consider the case of a binary input channel, i.e., $|\mathcal{X}| = 2$. The cardinality bound for channel prefixing V , is $|\mathcal{V}| \leq 2$.

A. The Scheme

Let $U^n = V^n G_n$. Consider the following sets:

$$\begin{aligned} \mathcal{H}_V &= \{i \in [n] : Z(U_i|U^{i-1}) \geq 1 - \delta_n\} \\ \mathcal{L}_V &= \{i \in [n] : Z(U_i|U^{i-1}) \leq \delta_n\}, \end{aligned} \quad (14)$$

$$\begin{aligned} \mathcal{H}_{V|Y} &= \{i \in [n] : Z(U_i|U^{i-1}, Y^n) \geq 1 - \delta_n\} \\ \mathcal{L}_{V|Y} &= \{i \in [n] : Z(U_i|U^{i-1}, Y^n) \leq \delta_n\}, \end{aligned} \quad (15)$$

$$\begin{aligned} \mathcal{H}_{V|Z} &= \{i \in [n] : Z(U_i|U^{i-1}, Z^n) \geq 1 - \delta_n\} \\ \mathcal{L}_{V|Z} &= \{i \in [n] : Z(U_i|U^{i-1}, Z^n) \leq \delta_n\}, \end{aligned} \quad (16)$$

where $\delta_n = 2^{-n^\beta}$ and $\beta \in (0, 1/2)$.

The set $[n]$ can be partitioned into the following four sets:

$$G_{Y \wedge Z} = \mathcal{H}_V \cap \mathcal{L}_{V|Y} \cap \mathcal{L}_{V|Z}, \quad (17)$$

$$G_{Y \setminus Z} = \mathcal{H}_V \cap \mathcal{L}_{V|Y} \cap \mathcal{L}_{V|Z}^c, \quad (18)$$

$$G_{Z \setminus Y} = \mathcal{H}_V \cap \mathcal{L}_{V|Y}^c \cap \mathcal{L}_{V|Z}, \quad (19)$$

$$B_{Y \wedge Z} = \mathcal{H}_V^c \cup (\mathcal{L}_{V|Y}^c \cap \mathcal{L}_{V|Z}^c). \quad (20)$$

From a successive decoding point of view, the sub-channels corresponding to the set $G_{Y \wedge Z}$ are simultaneously good for Bob and Eve. The sub-channels in the set $G_{Y \setminus Z}$ are good for Bob but bad for Eve. On the other hand, the sub-channels in the set $G_{Z \setminus Y}$ are good for Eve but bad for Bob. Last, the sub-channels in the set $B_{Y \wedge Z}$ are bad for both Bob and Eve.

Similar to (7)–(9), we have:

$$\begin{aligned} \mathcal{I}_Y &= \mathcal{H}_V \cap \mathcal{L}_{V|Y}, \\ \mathcal{I}_Z &= \mathcal{H}_V \cap \mathcal{L}_{V|Z}, \\ \mathcal{F}_r^Y &= \mathcal{H}_V \cap \mathcal{L}_{V|Y}^c, \\ \mathcal{F}_r^Z &= \mathcal{H}_V \cap \mathcal{L}_{V|Z}^c, \\ \mathcal{F}_d &= \mathcal{H}_V^c. \end{aligned} \quad (21)$$

By (11), we have

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{I}_Y| &= I(V; Y), \\ \lim_{n \rightarrow \infty} \frac{1}{n} |\mathcal{I}_Z| &= I(V; Z). \end{aligned} \quad (22)$$

For the *symmetric* and *degraded* wiretap channel [14]–[17], $G_{Z \setminus Y}$ is an empty set, since the degraded property of the channel causes $\mathcal{I}_Z \subset \mathcal{I}_Y$ [13]. However, for the general wiretap channel, $G_{Z \setminus Y}$ is no longer an empty set, and $|G_{Z \setminus Y}|$ cannot be negligible [18]–[20].

Here, we consider the positive secrecy capacity case, thus we have $|G_{Y \setminus Z}| > |G_{Z \setminus Y}|$. Choose a set, $C_{Y \setminus Z}$, such that $C_{Y \setminus Z} \subset G_{Y \setminus Z}$ and $|C_{Y \setminus Z}| = |G_{Z \setminus Y}|$. Define the set S as:

$$S = G_{Y \setminus Z} \setminus C_{Y \setminus Z}.$$

From (22), we have

$$\lim_{n \rightarrow \infty} \frac{1}{n} |S| = I(V; Y) - I(V; Z). \quad (23)$$

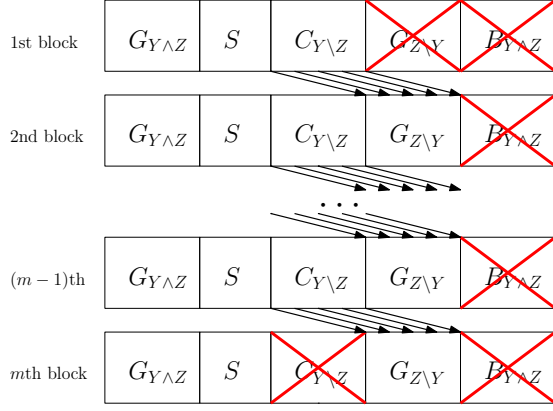


Fig. 1. Chaining construction.

We construct the code as follows. Consider an m -chain polar code in Definition 1. For $1 \leq i < m$, the set $C_{Y \setminus Z}$ in the i th block is chained to $G_{Z \setminus Y}$ in the $(i+1)$ th block as in Fig. 1. For each of the m blocks, the set $B_{Y \wedge Z}$ is set to be frozen. Moreover, the set $G_{Z \setminus Y}$ in the 1st block is set to be frozen in the sense that $G_{Z \setminus Y} \subseteq \mathcal{F}_r^Y$, and the set $C_{Y \setminus Z}$ in the m th block is also set to be frozen in the sense that $C_{Y \setminus Z} \subseteq \mathcal{F}_r^Z$. In Fig. 1, we use a red cross to denote a frozen set.

We put the secret information bits in the set S in each block. Therefore, the set S is used for secret message transmission. For blocks $1 \leq i < m$, we put uniformly distributed random bits to $C_{Y \setminus Z}$ to serve as the confusion messages. Through the chaining construction, the confusion messages are also chained to the set $G_{Z \setminus Y}$ in block $1 < i \leq m$. Moreover, the set $G_{Y \wedge Z}$ in each block are also filled with random bits to serve as confusion message. For the frozen sets, if the index belongs to \mathcal{F}_r^Y or \mathcal{F}_r^Z , then we put uniformly distributed random bits and share the randomness with the decoder (Bob and Eve). Last, if the index belongs to \mathcal{F}_d , then we determine the value according to the randomized map defined in (10). We summarize the encoding procedure as follows.

Encoding procedure:

For each block, the secret information bits are put in U_S , and determine the bits in $U_{\mathcal{F}_d}$ by (10).

For the 1st block,

- 1) Put uniformly distributed random bits to $U_{G_{Y \wedge Z} \cup C_{Y \setminus Z}}$.
- 2) Put uniformly distributed random bits to $U_{\mathcal{F}_r^Y}$, and share the randomness with the decoder.

For the j th block, $2 \leq j < m$,

- 1) Put uniformly distributed random bits to $U_{G_{Y \wedge Z} \cup C_{Y \setminus Z}}$.
- 2) Chaining construction: repeat the bits in $C_{Y \setminus Z}$ of the $(j-1)$ th block to the bits in $U_{G_{Z \setminus Y}}$.
- 3) Put uniformly distributed random bits to $U_{\mathcal{F}_r^Y \cap \mathcal{F}_r^Z}$, and share the randomness with the decoder.

For the m th block,

- 1) Put uniformly distributed random bits to $U_{G_{Y \wedge Z}}$.
- 2) Chaining construction: repeat the bits in $C_{Y \setminus Z}$ of the $(m-1)$ th block to the bits in $U_{G_{Z \setminus Y}}$.
- 3) Put uniformly distributed random bits to $U_{\mathcal{F}_r^Z}$, and share the randomness with the decoder.

Note that in the chaining construction we require the bits in $U_{G_{Z \setminus Y}}$ equal the bits in $U_{C_{Y \setminus Z}}$. Since we fill uniformly distributed random bits to $U_{C_{Y \setminus Z}}$, we simultaneously fill random bits to $U_{G_{Z \setminus Y}}$. Due to the fact that $G_{Z \setminus Y} \cap \mathcal{F}_d = \emptyset$, we can freely choose bits in this set.

Decoding procedure:

Bob decodes from the 1st block. In each block, if $i \in \mathcal{F}_d$, then $\hat{u}_i = \arg \max_{u \in \{0,1\}} P_{U_i|U^{i-1}}(u|\hat{u}^{i-1})$. For the 1st block,

$$\hat{u}_i = \begin{cases} u_i & \text{if } i \in \mathcal{F}_r^Y, \\ \arg \max_{u \in \{0,1\}} P_{U_i|U^{i-1}, Y^n}(u|\hat{u}^{i-1}, y^n) & \text{if } i \in G_{Y \wedge Z} \cup C_{Y \setminus Z} \cup S. \end{cases}$$

For the j th block, $2 \leq j < m$,

$$\hat{u}_i = \begin{cases} u_i & \text{if } i \in \mathcal{F}_r^Y \cap \mathcal{F}_r^Z, \\ \arg \max_{u \in \{0,1\}} P_{U_i|U^{i-1}, Y^n}(u|\hat{u}^{i-1}, y^n) & \text{if } i \in G_{Y \wedge Z} \cup C_{Y \setminus Z} \cup S, \\ \hat{u}_{i'} & \text{in the } (j-1)\text{th block, where } i' \in C_{Y \setminus Z} \\ \hat{u}_i & \text{if } i \in G_{Z \setminus Y}. \end{cases}$$

For the m th block,

$$\hat{u}_i = \begin{cases} u_i & \text{if } i \in \mathcal{F}_r^Z, \\ \arg \max_{u \in \{0,1\}} P_{U_i|U^{i-1}, Y^n}(u|\hat{u}^{i-1}, y^n) & \text{if } i \in G_{Y \wedge Z} \cup S, \\ \hat{u}_{i'} & \text{in the } (m-1)\text{th block, where } i' \in C_{Y \setminus Z} \\ \hat{u}_i & \text{if } i \in G_{Z \setminus Y}. \end{cases}$$

B. Reliability

From (23), we know as $n \rightarrow \infty$, our coding scheme can achieve the secrecy rate in (1). Moreover, when Bob applies the decoding procedure described in Sec. IV-A, according to (12), the block error probability of the whole m -chain block can be upper bounded by

$$P_e \leq (m-1) \sum_{i \in C_{Y \setminus Z}} Z(U_i|U^{i-1}, Y^n) + m \sum_{i \in G_{Y \wedge Z} \cup S} Z(U_i|U^{i-1}, Y^n) = O(2^{-n^\beta})$$

for any $\beta \in (0, 1/2)$ with complexity $O(n \log n)$. Therefore, the secrecy rate in (1) can be achieved reliably.

C. Equivocation Calculation

We first introduce necessary notation for the calculation of the equivocation rate. In the encoding process, we consider m blocks each with block length n . Let Z^{mn} denote what Eve receives. For each block, we perform $U^n = V^n G_n$, therefore, for the total of m blocks, we have V^{mn} and U^{mn} .

Let W_s denote the secret message, and \tilde{W}_s denote the confusion message. Let the subscript i of a set denote the set in the i th block. For example, S_i denotes the set S in the i th block, and $G_{Y \wedge Z_j}$ denotes the set $G_{Y \wedge Z}$ in the j th block. Since secret message is put in S_i , $1 \leq i \leq m$, we have $W_s = \cup_{1 \leq i \leq m} U_{S_i}$. Also, the confusion message is put

in $G_{Y \wedge Z_i}$, $1 \leq i \leq m$ and $C_{Y \setminus Z_j}$, $1 \leq j < m$. Therefore, we have $\tilde{W}_s = \cup_{1 \leq i \leq m, 1 \leq j < m} U_{G_{Y \wedge Z_i}} U_{C_{Y \setminus Z_j}}$.

We can calculate the equivocation rate as follows:

$$H(W_s | Z^{mn}) = H(W_s, \tilde{W}_s | Z^{mn}) - H(\tilde{W}_s | W_s, Z^{mn}) \quad (24)$$

$$= H(W_s, \tilde{W}_s) - I(W_s, \tilde{W}_s; Z^{mn}) - H(\tilde{W}_s | W_s, Z^{mn}) \quad (25)$$

$$\geq H(W_s, \tilde{W}_s) - I(V^{mn}; Z^{mn}) - H(\tilde{W}_s | W_s, Z^{mn}) \quad (26)$$

$$= H(W_s) + H(\tilde{W}_s) - I(V^{mn}; Z^{mn}) - H(\tilde{W}_s | W_s, Z^{mn}) \quad (27)$$

which is equivalent to

$$\frac{1}{mn} I(W_s; Z^{mn}) \leq \frac{1}{mn} I(V^{mn}; Z^{mn}) + \frac{1}{mn} H(\tilde{W}_s | W_s, Z^{mn}) - \frac{1}{mn} H(\tilde{W}_s). \quad (28)$$

Here, (24) is due to chain rule of conditional entropy, (25) is due to the definition of mutual information, (26) comes from the data processing inequality, (27) is due to the independence of the secret message and the confusion message. In (28), we bound each terms on the right hand side as follows:

For the first term, we have $I(V^{mn}; Z^{mn}) \leq \sum_1^{mn} I(V_i; Z_i) \leq mn I(V; Z)$. Therefore, $\frac{1}{mn} I(V^{mn}; Z^{mn}) \leq I(V; Z)$.

To bound the second term, suppose Eve obtains \tilde{W}_s and Z^{mn} , and wants to decode \tilde{W}_s . By symmetry of chaining construction, Eve can apply similar decoding rule as described in Sec. IV-A. However, this time Eve decodes from the m th block, then the block error probability of the whole m -chain block can be upper bounded by

$$P_e \leq (m-1) \sum_{i \in G_{Z \setminus Y}} Z(U_i | U^{i-1}, Y^n) + m \sum_{i \in G_{Y \wedge Z}} Z(U_i | U^{i-1}, Y^n) = O(2^{-n^\beta})$$

for $\beta \in (0, 1/2)$. Hence, by applying Fano's inequality, we have

$$H(\tilde{W}_s | W_s, Z^{mn}) \leq H(P_e) + P_e \log |\tilde{W}_s| < H(P_e) + P_e [mn I(V; Z)].$$

Therefore, as $n \rightarrow \infty$, $\frac{1}{mn} H(\tilde{W}_s | W_s, Z^{mn}) \rightarrow 0$.

For the last term, as $n \rightarrow \infty$, by (13) and (22), we have $(m-1)n I(V; Z) < H(\tilde{W}_s) < mn I(V; Z)$. Hence, as $m \rightarrow \infty$, $\frac{1}{mn} H(\tilde{W}_s) \rightarrow I(V; Z)$.

After we bound the right hand side of (28), we know as $n \rightarrow \infty$ and $m \rightarrow \infty$, $\frac{1}{mn} I(W_s; Z^{mn}) \rightarrow 0$. Therefore, the weak secrecy constraint is achieved.

V. CONCLUSION

We proposed a polar coding scheme that achieves the secrecy capacity of the general wiretap channel, by using the chaining construction technique and polar coding for asymmetric channels. Compared to previous work, our construction has better decoding error probability and can be constructed more efficiently. Finally, we note that this chaining construction based polar coding scheme can be extended to achieve *strong* secrecy guarantees as presented in [30].

REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [3] E. Arkan, "Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.
- [4] —, "Source polarization," in *IEEE ISIT*, Jun. 2010.
- [5] S. Korada and R. Urbanke, "Polar codes are optimal for lossy source coding," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1751–1768, Apr. 2010.
- [6] E. Şaşoğlu, İ. E. Telatar, and E. Yeh, "Polar codes for the two-user multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6583–6592, Oct. 2013.
- [7] E. Abbe and İ. E. Telatar, "Polar codes for the m -user multiple access channel," *IEEE Trans. Inf. Theory*, vol. 58, no. 8, pp. 5437–5448, Aug. 2012.
- [8] S. Öney, "Successive cancellation decoding of polar codes for the two-user binary-input mac," in *IEEE ISIT*, Jul. 2013.
- [9] N. Goela, E. Abbe, and M. Gastpar, "Polar codes for broadcast channels," Jan. 2013. [Online]. Available: <http://arxiv.org/abs/1301.6150v1>
- [10] M. Mondelli, S. H. Hassani, I. Sason, and R. Urbanke, "Achieving Marton's region for broadcast channels using polar codes," Feb. 2014. [Online]. Available: <http://arxiv.org/abs/1401.6060v2>
- [11] L. Wang and E. Şaşoğlu, "Polar coding for interference networks," Jan. 2014. [Online]. Available: <http://arxiv.org/abs/1401.7293>
- [12] E. Arkan, "Polar coding for the Slepian-Wolf problem based on monotone chain rules," in *IEEE ISIT*, Jul. 2012.
- [13] S. B. Korada, "Polar codes for channel and source coding," Ph.D. dissertation, EPFL, May 2009.
- [14] H. Mahdaviifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.
- [15] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Comm. Letters*, vol. 14, no. 8, pp. 752–754, Aug. 2010.
- [16] O. O. Koyluoglu and H. E. Gamal, "Polar coding for secure transmission and key agreement," in *IEEE PIMRC*, Sep. 2010.
- [17] E. Hof and S. Shamai, "Secrecy-achieving polar-coding," in *IEEE ITW*, Aug. 2010.
- [18] S. Hassani, S. Korada, and R. Urbanke, "The compound capacity of polar codes," in *Allerton Conf.*, Sep. 2009.
- [19] I. Tal and A. Vardy, "How to construct polar codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6562 – 6582, Oct. 2013.
- [20] D. Sutter and J. M. Renes, "Universal polar codes for more capable and less noisy channels and sources," Apr. 2014. [Online]. Available: <http://arxiv.org/abs/1312.5990v3>
- [21] S. H. Hassani and R. Urbanke, "Universal polar code," Dec. 2013. [Online]. Available: <http://arxiv.org/abs/1307.7223v2>
- [22] E. Şaşoğlu and L. Wang, "Universal polarization," Dec. 2013. [Online]. Available: <http://arxiv.org/abs/1307.7495v2>
- [23] J. Honda and H. Yamamoto, "Polar coding without alphabet extension for asymmetric models," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 7829–7838, Dec. 2013.
- [24] D. Sutter, J. M. Renes, and R. Renner, "Efficient one-way secret-key agreement and private channel coding via polarization," Apr. 2013. [Online]. Available: <http://arxiv.org/abs/1304.3658>
- [25] O. Ozel and S. Ulukus, "Wiretap channels: implications of the more capable condition and cyclic shift symmetry," *IEEE Trans. Inf. Theory*, vol. 59, no. 4, pp. 2153–2164, Apr. 2013.
- [26] E. Şaşoğlu and İ. Telatar, "Polarization for arbitrary discrete memoryless channels," in *IEEE ITW*, Oct. 2009.
- [27] R. Mori and T. Tanaka, "Channel polarization on q -ary discrete memoryless channels by arbitrary kernel," in *IEEE ISIT*, Jun. 2010.
- [28] E. Şaşoğlu, "Polar codes for discrete alphabets," in *IEEE ISIT*, Jul. 2012.
- [29] W. Park and A. Barg, "Polar codes for q -ary channels, $q = 2^r$," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 955–969, Feb. 2013.
- [30] E. Şaşoğlu and A. Vardy, "A new polar coding scheme for strong security on wiretap channels," in *IEEE ISIT*, Jul. 2013.